Deloitte.

The Digital Policing Journey: From Concept to Reality
Realising the benefits of transformative technology

Foreword

The founding principles of policing, as defined by Sir Robert Peel, are as true and necessary today as they *ever* were. But the realities and pressures of the 21st century call for a new, digital way of operating.

Today the UK police service is at a tipping point. Police forces face increasing public expectations and scrutiny, changes in crime profile and increasing non-crime-related demand. They must deliver improved services despite facing the deepest budget cuts in a generation, as the austerity measures are likely to continue until at least 2019. There is increasing pressure to deliver more – for less.

As both criminal activity and interaction with citizens move increasingly online, the traditional model of providing a physical presence in order to deter crime and reassure communities is no longer enough on its own, and is costly too. Police forces must learn to harness digital technology if they are to deliver a service that is fit for purpose in the 21st century.

Digital technology has the potential to transform the way policing is delivered – taking police officers away from police stations and bringing them closer to communities and crime spots. However, in order to truly benefit from these new digital capabilities a holistic approach is required – starting with core processes and behaviours. In realising the potential of digital technologies police forces can learn from private sector organisations that share similar characteristics and challenges: a mobile workforce; the need to process and analyse vast amounts of data to make decisions, and operationalise those decisions quickly; the need to engage with customers via multiple channels; the ability to respond to customers' desire for self-service.

In this paper we present the concept of digital policing across the lifecycle of crime prevention, response and investigation. We then look at how forces can learn from the successes and failures of the private sector to make this concept a reality. Over the past decade Deloitte has helped many consumer-facing organisations embed digital ways of operating, and we have summarised the common pitfalls and success factors here.

Successfully adopting digital technologies requires a holistic view of policing operations. This paper provides practical recommendations in five key steps. It looks at processes, information, systems, devices and location.

Our future digital police service will not only be more efficient in fighting crime – but much more powerful too.

James Taylor
Partner

Traditional policing objectives have not changed, but the current ways of delivering services are becoming outdated

Policing principles have seen little change since 1829. As outlined in the 'National Policing Vision 2016' by the College of Policing, forces still exist primarily to prevent crime and protect the public.

Originally, police forces relied heavily on the decision-making abilities of individual officers and their physical proximity to crime hotspots.

The technology revolution of the 1970s and 1980s enabled a more informed decision-making process, based on the information held and analysed in computer systems. But it also meant officers spending large amounts of time at police stations, where computers took them away from where their services were required most.

Today digital technologies make it possible for police officers to be *where* crime is happening, *when* it is happening – even in virtual locations.

Their actions can then be directed by powerful, instantly available insights, based on the analysis of vast amounts of data. The location and time of criminal activity can now be identified – or even predicted – faster. So officers can return to the streets, and, thanks to digital technology, be better equipped with information to support their decisions.

However, policing is still reliant on 'old-school' infrastructure and processes: extensive networks of police stations, manual processing of intelligence, face-to-face briefings, paper-based case files and forensic capabilities focussed on physical evidence.

Without deploying digital technology, the task of fighting crime and protecting citizens becomes almost impossibly tough in a world where citizens and criminals alike are increasingly digitally savvy. Failure to adopt digital technologies also restricts the ability of police forces to operate effectively within the ever more constrained budgets driven by the Comprehensive Spending Reviews.

The importance of digital has also been highlighted by Her Majesty's Inspectorate of Constabulary's ongoing inspections into how forces are dealing with cybercrime and maximising the opportunities offered by digital technologies.

Today digital technologies make it possible for police officers to be *where* crime is happening, *when* it is happening – even in virtual locations.

Police forces can transform the delivery of their services by applying technologies that have been tried and tested in the private sector

Private sector enterprises use digital technologies to maximise the time their workforces spend on delivering core services and meeting customer needs. The services of consumer businesses have been transformed by predictive analytics, digital customer interaction channels, dynamic scheduling of field forces, mobile communications, and remote access to core information systems.

The four lenses of Digital Policing

If applied to policing, digital technologies can push the boundaries of what is possible across four lenses:

Proactive policing	**Digital engagement and digital contact management**	**Mobile workforce optimisation**	**Digital investigation**
Deterring criminal activity through proactive action, driven by data analytics and evidence-based policing.	Includes multi-channel communication with the public, online crime reporting and crowd-sourced intelligence, investigation via social media platforms, and digital channels for low-risk contact with the police. All these services can reduce demand on control rooms and contact centres.	Neighbourhood and response officers patrolling the beat more regularly, enabled by mobile devices which they can use to receive and deliver tasking and intelligence, search internal systems, capture statements and record supporting evidence.	Digital case files containing evidence and the latest forensics, developed and edited by multiple officers on the move and shared in real time with the Crown Prosecution Service.

Applying digital technologies across these four lenses can enable police forces to use their resources more intelligently, target criminal activity more proactively, and deliver a faster, more targeted response through real-time information-sharing and effective decision-making.
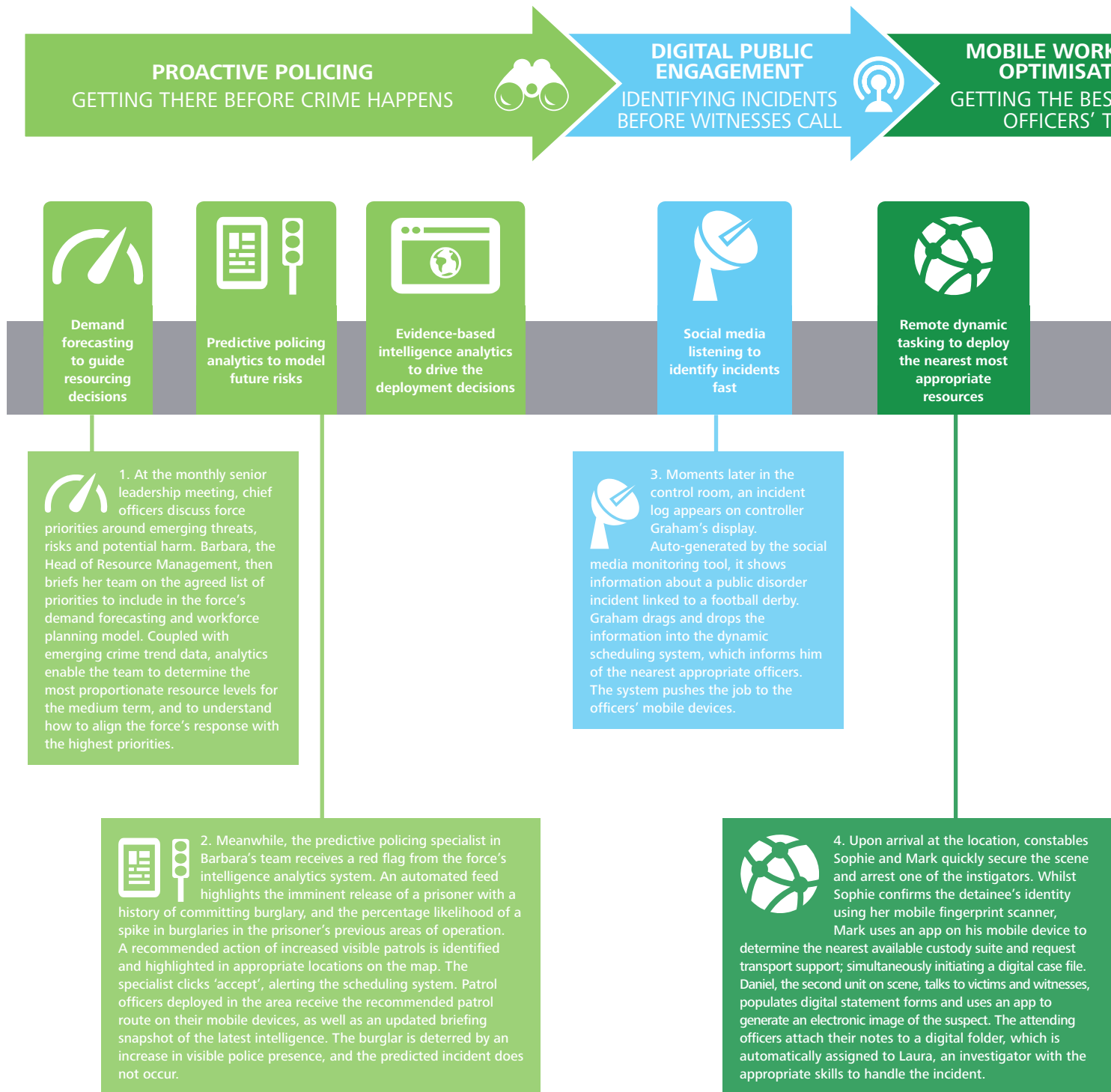
Experience from the Private Sector

Private sector experience presents multiple examples of how digital technologies can support increased efficiency of operations and improved customer engagement, including:

- **Workforce mobility:** Utility companies increasingly rely on real-time scheduling technology for automated tasking to their engineers. Tasks are assigned based on the engineers' skillsets and proximity to the customer, ensuring the most efficient routes are taken. Consumer businesses push tasks and information about new offers out to their field sales representatives' mobile devices to enable them to adapt their sales strategies real-time.

- **Social media listening:** Global entertainment corporations monitor global social media feeds to determine sentiment, breadth and influence of posts and links these to revenue generated by new films.

- **Self-service channels:** Orders in the fast moving consumer goods industry can be managed through online portals or mobile apps, accessible to sales representatives, contact centre staff and customers.

- **Crowdsourcing:** Consumer goods companies increasingly involve their customers in new product development and social media campaigns.

- **Big data analytics:** Insurance companies analyse consumer data to determine the best treatment strategies that are personalised for each customer.

- **Social media collaboration tools:** Some transnational corporations have introduced 'collaboration tools' to encourage cooperation around revenue generating opportunities across their global business networks.

- **Next best action:** Financial services companies, telecommunications and utilities use business rules engines to determine the next best action in treating specific customers based on the customer information, context and nature of enquiry.

The Digital Policing Scenario

These four lenses are demonstrated in our digital policing scenario. Here we redefine the reality of contemporary policing by applying digital technologies that have been tried and tested in the private sector.

PROACTIVE POLICING
GETTING THERE BEFORE CRIME HAPPENS

DIGITAL PUBLIC ENGAGEMENT
IDENTIFYING INCIDENTS BEFORE WITNESSES CALL

MOBILE WORK OPTIMISAT
GETTING THE BES OFFICERS' T

Demand forecasting to guide resourcing decisions

Predictive policing analytics to model future risks

Evidence-based intelligence analytics to drive the deployment decisions

Social media listening to identify incidents fast

Remote dynamic tasking to deploy the nearest most appropriate resources

1. At the monthly senior leadership meeting, chief officers discuss force priorities around emerging threats, risks and potential harm. Barbara, the Head of Resource Management, then briefs her team on the agreed list of priorities to include in the force's demand forecasting and workforce planning model. Coupled with emerging crime trend data, analytics enable the team to determine the most proportionate resource levels for the medium term, and to understand how to align the force's response with the highest priorities.

3. Moments later in the control room, an incident log appears on controller Graham's display. Auto-generated by the social media monitoring tool, it shows information about a public disorder incident linked to a football derby. Graham drags and drops the information into the dynamic scheduling system, which informs him of the nearest appropriate officers. The system pushes the job to the officers' mobile devices.

2. Meanwhile, the predictive policing specialist in Barbara's team receives a red flag from the force's intelligence analytics system. An automated feed highlights the imminent release of a prisoner with a history of committing burglary, and the percentage likelihood of a spike in burglaries in the prisoner's previous areas of operation. A recommended action of increased visible patrols is identified and highlighted in appropriate locations on the map. The specialist clicks 'accept', alerting the scheduling system. Patrol officers deployed in the area receive the recommended patrol route on their mobile devices, as well as an updated briefing snapshot of the latest intelligence. The burglar is deterred by an increase in visible police presence, and the predicted incident does not occur.

4. Upon arrival at the location, constables Sophie and Mark quickly secure the scene and arrest one of the instigators. Whilst Sophie confirms the detainee's identity using her mobile fingerprint scanner, Mark uses an app on his mobile device to determine the nearest available custody suite and request transport support; simultaneously initiating a digital case file. Daniel, the second unit on scene, talks to victims and witnesses, populates digital statement forms and uses an app to generate an electronic image of the suspect. The attending officers attach their notes to a digital folder, which is automatically assigned to Laura, an investigator with the appropriate skills to handle the incident.

**KFORCE
TION**
**T OUT OF
IME**

DIGITAL INVESTIGATION
ACCELERATING THE INVESTIGATION THROUGH
REAL-TIME INFORMATION EXCHANGE

Mobile booking of custody and additional support

Electronic witness statement & electronic suspect image

Mobile digital case file with real-time sharing and digital evidence capture

Mobile ID verification and multi-system search in custody

Crowd-sourced investigation through social media

Digitised collaboration with CPS and court proceedings

5. Receiving an automated prompt that her next case is on the system, Laura opens the folder and uploads relevant content to a social media platform to crowd-source information that could be of use for the investigation.

6. Just before the detainee is brought into custody, the new record appears on detention officer Charles's screen of the custody management system, based on the results of the remote ID verification. An automated search of multiple systems has been completed, and no known matches identified. Charles confirms an automated message to be sent to the suite's mental health liaison for any known information relevant to the suspect's detention, and proceeds with the booking-in process.

8. Laura completes the digital case file and works remotely with colleagues to prepare the court folder, collaborating in real-time with the Crown Prosecution Service via the designated mobile app to ensure the court folder meets requirements and the evidence provided is sound. The case results in convictions for the two men involved. Laura updates the case file, and her colleagues are automatically notified of changes to the shared document.

7. That afternoon, investigator Laura logs on to the social media platform to see if anyone has provided any information about the public disorder incident. A member of the public has provided a name. A quick search of the system informs her that the additional suggested suspect is wanted for drug dealing and Laura coordinates with the proactive investigation team. An operation is soon planned and executed, leading to a successful arrest and seizure.

Many police forces in England and Wales have invested in digital technologies. Private sector experience provides insight into maximising success

According to the National Audit Office 'Mobile Technology in Policing' report, a number of factors led forces to introduce a range of technologies very quickly, which resulted in "increased costs, high levels of maintenance and a significant training commitment".

Many organisations that have tried to go digital have been slow to realise the full benefits. From our experience of digital projects in the private sector, we have identified a number of opportunities that help organisations maximise the potential benefits.

Focusing on requirements, not devices
When investing in digital technology, the most common mistake businesses make is buying and equipping their workforce with mobile devices without considering a full range of requirements or the processes that those devices need to support.

Similarly, businesses often buy technology solutions with a single issue in mind, rather than taking a holistic view of strategy and IT architecture.

This focus on buying devices to resolve an isolated business issue often results in an over-equipped workforce using conflicting technologies, as well as significant purchase, maintenance and training costs.

Using data to generate insight
Digital technologies enable the processing of large volumes of information to provide actionable insight and deliver this information remotely and in real time to those who need it. But this rich opportunity is often undermined by the complex webs of legacy systems and complicated information flows that can underpin business-critical processes.

Remembering the users
According to the latest Deloitte CIO survey, 83% of respondents believe that resistance by employees is the main reason for the failure of IT projects.

While in the private sector resistance from the field is an issue, in policing, frontline officers actually often drive the introduction of mobile devices. But even so, adoption commonly still falters because of a failure to provide the right information on the mobile devices that supports officers in their daily jobs.

Focusing on victims and citizens is vital
Our research, 'Making digital default', shows that 88 per cent of citizens are keen to engage online. But government needs to build trust and offer services that are so well designed that people proactively choose them over the alternative. Assisted digital and traditional channels will still be essential for some communities and vulnerable citizens too.

From our experience of digital projects in the private sector, we have identified a number of opportunities that help organisations maximise the potential benefits.

To successfully go digital, police forces need to adopt a holistic view of their operations and change the way they deliver their core services

As the Minister for Policing stated during the College of Policing's Digital Pathfinders conference:

"Transformative use of IT is pivotal to these changes , but business change – doing things differently – is also critical. This is about transforming how policing is done in a digital world and not just digitising inefficient analogue processes." Damian Green, Minister of State for Policing and Criminal Justice

Simply procuring devices does not guarantee a successful digital transformation. It requires a holistic view of the organisation – including processes, information, technology and people. Based on the lessons learned from the private sector, these five steps will help in introducing digital effectively:

1. Create new processes, don't just re-design it

Rather than starting with system or device selection, an effective approach to introducing digital technologies brings together three different perspectives: the strategic view of how operational processes need to change, an 'art-of-the-possible' view based on emerging technologies, and a user experience view.

Focusing on the first of these, using the functionality of leading technologies to support existing force processes will not fix problems, and can often lead to unnecessary disruption without delivering any clear benefits. Digital solutions – such as digital case files, data analytics, automated process management and remote monitoring or dynamic scheduling – can transform the way forces operate, but must be preceded by the introduction of the new processes that they will eventually support.

For example, police forces already own vast quantities of powerful data that is often manually processed by intelligence departments and verbally transferred to frontline officers in daily briefings. Data analytics enables such information to be examined automatically, with real-time actionable insight generated that can be used to support intelligence-led policing. Analytics can be combined with robust business rules to support longer-term demand forecasting and so in resource planning too; moving the emphasis to crime prevention over response.

2. Think about the information first, then systems

Once the future processes have been designed, forces need to identify what information is required to enable them. They also need to ensure the available information is of sufficient quality to be used with confidence.

The main barriers to utilising more information to optimise police operations are (a) Managing new and increased volumes of data, and the effort required to analyse this; and (b) difficulties in effectively integrating data that has come from a multitude of sources, including legacy systems.

Technologies available today can help automate data analysis and enable real-time decision making, turning information into a powerful tool. A key enabling factor here is information architecture: a clear view of all the information items required for each process and the locations from which they are sourced. Information architecture designed around business objectives and process needs can help ensure the quality of data and make the most of the information that is gathered and created within the organisation. In defining the information architecture, it is important to design governance that will ensure data quality, while at the same time allowing sharing of information, as opposed to locking it down unnecessarily.

3. Create flexible systems architecture

After confirming the requirements associated with new processes and conducting an information analysis, necessary system functionality can be identified and the most appropriate technologies selected.

Flexibility should be the key feature of modern police systems architecture. Every officer and member of staff in a force can gather and develop valuable information, so trying to enforce the use of a single centralised system to capture this information in a standardised way in an organisation that relies on independent thinking is likely to fail. Factor in the ever-changing nature of external sources of information and the ways in which crimes are committed, and it becomes clear that systems architecture must be a constantly evolving concept. A structure is needed that can flexibly switch on and off a variety of internal and external systems and devices without breaking the integrity of the wider information architecture.

A new approach to data security is required to enable the police systems architecture to access multiple sources, and enable remote real-time information exchange. Whilst integrity should remain central to service delivery, many existing security requirements are outdated. In addition, the security of the core technology platform needs to become more robust to support the secure remote exchange of sensitive data.

4. Select the right range of devices and create a user-friendly interface

The technology marketplace moves very quickly. Selecting a device-agnostic platform is important for future-proofing a force whilst still identifying the right balance of devices required to meet its specific needs. Users should be involved in the selection of devices, as gaining their approval can make or break a force's digital programme. Initial process analysis (as outlined in step one) will have identified useful apps to offer and involving the users in designing their experience will help ensure officers and staff are using the devices effectively in their daily work.

5. Don't let base location drive officer deployment

With real-time mobile access to all required information and the capability for remote briefings, there is no need for police officers to be tied to a base location. Dynamic scheduling technology can enable the most efficient use of officers' time and send the right resources to the right jobs in the right locations, minimising the need for office-based command and control staff.
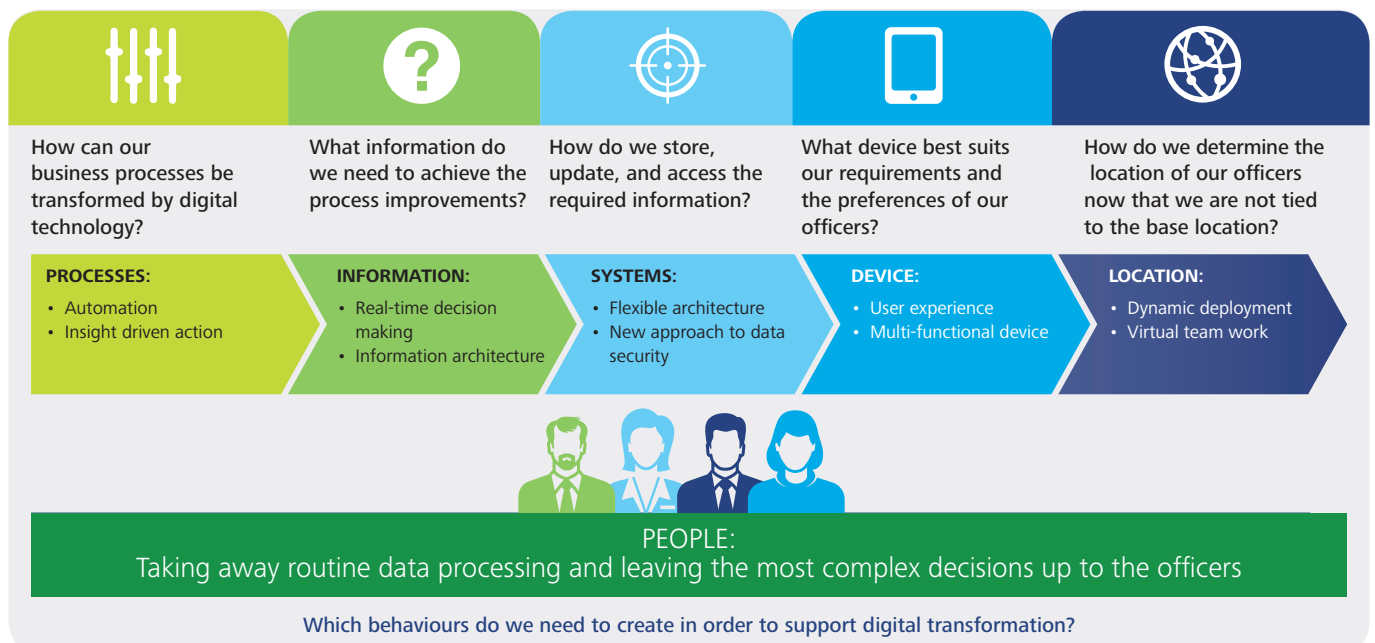
So officers can be present where crime happens, even before it happens – and where their services are in highest demand from the people they serve. Remote access to systems also means that back-office staff can be home-based and work in virtual teams, creating a more inclusive and flexible working environment and extending the recruitment pool.

At every step of your digital policing programme, think about the people.

Key decisions within operational policing will always be made by operational police officers and staff. The fundamental role of human instinct, emotional intelligence and pragmatic decision-making in policing must be recognised in designing digital. However, this role will become slightly different, and this will also need due consideration. Digital policing will, in effect, require a new breed of police officers. The notions of the 'station', 'beat' and 'beat sergeant' will be eroded. A digital police officer will have instant mobile access to intelligence, combined with a contextual view enabled by being close to crime spots. This will often mean they are in a better position to make tactical decisions than their office-based supervisors. These new digital police officers need to be briefed, tasked and managed in a different way, marking a significant change in culture and ways of working that will require careful planning and time to 'bed in'.

In short, for police forces 'digital' is about helping officers serve the public more effectively, enabling them to spend more time on problem-solving, providing them with the information required to make intelligent decisions faster , more effectively, and in greater depth, and connecting staff to work more collaboratively. Having this service on a shiny tablet is just a finishing touch.

Five steps to introducing digital technology

PROCESSES:	INFORMATION:	SYSTEMS:	DEVICE:	LOCATION:
How can our business processes be transformed by digital technology?	What information do we need to achieve the process improvements?	How do we store, update, and access the required information?	What device best suits our requirements and the preferences of our officers?	How do we determine the location of our officers now that we are not tied to the base location?
• Automation • Insight driven action	• Real-time decision making • Information architecture	• Flexible architecture • New approach to data security	• User experience • Multi-functional device	• Dynamic deployment • Virtual team work

PEOPLE:
Taking away routine data processing and leaving the most complex decisions up to the officers

Which behaviours do we need to create in order to support digital transformation?

Contacts

James Taylor
Partner
020 7007 9721
jmtaylor@deloitte.co.uk

Lee Simpson
Senior Manager
020 7303 3037
leesimpson@deloitte.co.uk

Varvara Sidorova
Manager
020 7007 5993
vsidorova@deloitte.co.uk